

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS - EASTERN DIVISION**

JACINTA CASTRO AND SERAPIO CHAVEZ,
individually and on behalf of Themselves and all
other similarly situated persons, known and unknown,

Plaintiff(s),

v.

EL-MILAGRO, INC.,

Defendant.

Hon. Thomas M. Durkin

Case No.: 2022-cv-03943

AMENDED CLASS ACTION COMPLAINT

Plaintiffs, Jacinta Castro and Serapio Chavez (“Plaintiffs”) individually and on behalf of themselves and all other similarly situated persons, known and unknown (the “Proposed Class”), by their attorneys, Daniel I. Schlade and James M. Dore of Justicia Laboral, LLC, complains against Defendant El Milagro, Inc. (“Defendant”) and in support of this Complaint, states:

Introduction and Parties

1. This class action seeks redress for Defendant’s willful violations of the Illinois Biometric Information Privacy, Act, 740 ILCS 14/1, *et, seq.* (“BIPA”) for failure to comply with Illinois’s requirements for gathering individuals’ biometric data.
2. Plaintiffs are residents of Chicago, Illinois; and they are or were employed by Defendant.
3. Defendant El Milagro, Inc. is a corporation in the business of tortilla manufacturing, including in Chicago, Illinois. During relevant periods, upon information and belief, Defendant employed in excess of 250-500 different employees.

4. The Court possesses general subject matter jurisdiction over the state law BIPA claim. Jurisdiction is proper under 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendants are doing business within this State and because Plaintiff's and the Proposed Class's (the "Class") claims arise out of Defendant's unlawful in-state actions, as Defendant failed to comply with BIPA while taking Plaintiff and the Class's biometric information without complying with BIPA's requirements.

5. Venue is proper in the District Court of Illinois because all or most underlying facts and transactions occurred in Chicago, Illinois, and Plaintiffs reside in Chicago, and Defendants transact business in Chicago, Illinois.

COUNT I

Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq

6. Plaintiffs reincorporate by reference Paragraphs 1 through 5, as if set forth in full herein for Paragraph 6.

7. BIPA defines a "Biometric Identifier" as any personal feature that is unique to an individual, including fingerprints, palm scans, and face/facial feature/retinal scans. "Biometric information" is any information based on a biometric identifier, regardless of how it is converted or stored. 740 ILCS § 14/10. Collectively, biometric identifiers and biometric information are known as "biometrics".

8. This count concerns the taking and/or misuse of individuals' biometrics by Defendant El Milagro, Inc.

9. Defendant was and/or is capturing, storing, using, and/or disseminating the Biometric Information of Plaintiffs and other Class members without their informed written consent as required by law.

10. Defendant's biometric technology captures, collects, or otherwise uses Biometric Information, or portions and/or data derived therefrom, to authenticate the identity of individuals including Plaintiffs and members of the proposed class.

11. Biometric technology allows companies to reduce timekeeping fraud and/or acquire other efficiencies for their business. Unfortunately, along with the increased utility of biometric technology, so too come grave privacy risks associated with the unauthorized or malicious dissemination of this information.

12. The risk of harm is greatly magnified when biometrics are obtained in violation of reasonable regulations designed to protect individuals' irreplaceable information. The permanent and irreplaceable nature of one's biometrics makes the illegal collection of the same a significant public problem with far-reaching consequences, including irreversible identity theft.

13. Recognizing the irreversible harm presented by allowing the unregulated collection and use of biometrics, Illinois passed the BIPA, a statute addressing the collection, use, retention, possession, and dissemination of biometrics by private entities, such as Defendant El-Milagro, Inc..

14. Under BIPA, a biometric system, such as Defendant's system, is legal if, and only if, Defendant first:

(1) informs the person whose biometrics are to be collected in writing that biometric identifiers or biometric information will be collected or stored;

(2) informs the person whose biometrics are to be collected in writing of the specific purpose and the length of term for which such biometric identifiers or biometric information is being collected, stored and used;

(3) receives an executed written release from the person whose biometrics are to be collected, allowing the capture and collection of their biometric identifiers or biometric information; and

(4) publishes publicly available retention guidelines for permanently destroying biometric identifiers and biometric information. 740 ILCS 14/15(a).

15. Compliance with BIPA is straightforward and may be accomplished through a single, signed sheet of paper. BIPA's requirements bestow a right to privacy in biometrics and a right to make an informed decision when electing whether to provide or withhold biometrics.

16. At the time the BIPA was passed in 2008, another data privacy statute, the Personal Information Protection Act, 815 ILCS § 530 et seq. ("PIPA"), had been law in Illinois since 2006. PIPA provided a private right of action if a company possessing an individual's unique biometric data (the same data regulated by the BIPA) suffers a data security breach and fails to give affected consumers proper notice of such a breach. Further, numerous state and federal statutes, including the Illinois Consumer Fraud Act, also provide consumers a remedy in the event of an actual breach.

17. Defendant's biometric timekeeping system works by extracting biometric information from individuals, such as fingerprints, handprints, or portions thereof; and subsequently using the same for authentication and timekeeping purposes. The system includes the dissemination of biometrics to third parties, such as data storage vendors and payroll services. The biometrics are stored and repeatedly used each time a worker "clocks in" or "out" on the job.

18. The Illinois Legislature has found that "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, even sensitive information like Social Security numbers, when compromised, can be changed. Biometrics,

however, are biologically unique to each individual and therefore, once compromised, such individual has no recourse, is at a heightened risk for identity theft in, and is likely to withdraw from biometric facilitated transactions.” 740 ILCS 14/5. The risk is compounded when a person’s biometric information is also associated with his/her Social Security Number and potentially other relevant financial information or personal identifiable information. The gravity of the unresolvable problems created in the event of a data breach is so severe that the unlawful collection of such information constitutes actual harm.

19. Plaintiffs bring this action for damages and other remedies resulting from the actions of Defendant in capturing, storing, using, and disseminating his/her biometrics, and those other individuals throughout the state of Illinois, without informed written consent, and without informing them through a publicly available policy of how and when the subject biometrics would be stored or disposed of, in direct violation of the Illinois BIPA.

20. To the extent Defendant is still retaining Plaintiffs’ biometrics, such retention is unlawful. Plaintiffs would not have provided their biometric data to Defendant or utilized its biometric timekeeping technology had they known the same would remain with Defendant for an indefinite period or subject to unauthorized disclosure.

21. On behalf of themselves and the proposed Class defined below, Plaintiffs seek an injunction requiring Defendant to comply with BIPA, as well as an award of statutory damages to the Class members and common law monetary damages to be determined at trial, together with costs and reasonable attorneys’ fees.

22. During the relevant time, Plaintiffs worked at Defendant’s premises.

23. Defendant uses biometric scanning technology to monitor and track its employees' and other staffers, including Plaintiffs' time.

24. For the time period of years 2000 until 2023 of Plaintiffs' employment at Defendant's facilities, they were required to scan their fingerprints and/or other biometrics into Defendant's biometric timekeeping device each time they needed to "clock-in" and "clock-out". The system ensures that Plaintiffs could only verify their attendance and timeliness using the device. Defendant was aware that Plaintiffs and other Class members would be required to utilize the biometric timekeeping technology.

25. Plaintiffs relied on Defendant to not only provide a lawful and legally compliant system, but to also disclose all material information regarding the technology and system, including retention, destruction, and dissemination policies.

26. Defendant was aware, or reckless in failing to be aware, that its employees and staffers would be subject to its biometric technology. Defendant was aware that its biometric technology would be capturing, collecting, utilizing, and/or disseminating the biometrics of Plaintiffs and the Class members.

27. Defendant's biometric technology allows for and resulted in the dissemination of Plaintiffs and other Class member's biometrics to third parties, including vendors for timekeeping, data storage, and payroll purposes.

28. Prior to taking Plaintiffs' biometrics through its biometric technology, Defendant did not inform Plaintiffs in writing that their biometrics were being collected, stored, used, or disseminated, or publish any policy specifically about the collection, retention, use, deletion, or

dissemination of biometrics. Defendant did not seek, and Plaintiffs never provided, any executed written consent relating to the collection, use, storage, or dissemination of his biometrics.

29. Prior to taking Plaintiffs' biometrics, Defendant did not make publicly available any written policy as to a biometric retention schedule and guidelines for permanently destroying the collected biometrics.

30. Additionally, Defendant did not obtain written consent from Plaintiffs for the dissemination of their biometrics to third parties.

31. To this day, Plaintiffs are unaware of the status of their biometrics obtained by Defendant. Defendant has not informed Plaintiffs whether it still retains their biometrics, and if it does, for how long it intends to retain such information without his consent.

32. Plaintiffs and/or members of the Class have been aggrieved as a result of Defendant's violations of BIPA, and they may have suffered pecuniary damages in the form of lost wages, diminution in the unique identifying value of his biometrics, and other costs associated with identity protection.

33. Furthermore, Plaintiffs biometrics are economically valuable and such value will increase as the commercialization of biometrics continues to grow. Defendant's repeated use of Plaintiffs' biometrics does and will continue to confer a benefit on Defendant for which Plaintiffs was not sufficiently compensated.

34. At the time Plaintiffs biometrics were captured, Defendant did not have a publicly available policy of informing individuals, including Plaintiffs, of what happens to their biometrics after they are captured, whether the information is disseminated to a third party and, if so, which third party, and what would happen to the data if Defendant was to be acquired or file bankruptcy.

35. Plaintiffs and/or members of the Class have been aggrieved by Defendant's violation of BIPA, since Plaintiffs were denied the written disclosures, releases and other information required by Section 15 of BIPA, and thus Plaintiffs and/or members of the Class were deprived of: informed consent with respect to the taking of their biometric data; access to Defendant's biometric privacy policies; and/or other such rights afforded by BIPA.

36. By failing to comply with BIPA, Defendant has violated Plaintiffs' substantive state rights to biometric information privacy. Each and every instance that Defendants took Plaintiffs' and members of the proposed class's Biometric Information constituted a violation of BIPA. Pursuant to Section 20 of the BIPA, Defendant is liable to Plaintiffs for \$1,000.00 for each and every negligent violation of the BIPA; and \$5,000.00 for each and every intentional or reckless violation of the BIPA. Likewise, Defendant is liable to each member of the proposed class for \$1,000.00 for each and every negligent violation of the BIPA; and \$5,000.00 for each and every intentional or reckless violation of the BIPA.

Class Allegations

37. Plaintiffs brings this action on behalf of themselves and similarly situated individuals pursuant to 735 ILCS § 5/2-801. Plaintiffs seeks to represent a Class defined as follows:

Class: All of El Milagro, Inc.'s current and former employees or agents and staffers whose Biometric Information were captured, collected, stored, used, transmitted, or disseminated by or on behalf of Defendant or its technology within the State of Illinois any time within the applicable limitations period

38. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officers or directors.

39. Upon information and belief, there are at least 250-500 members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiffs, the members can be easily identified through Defendant's personnel records.

40. Plaintiffs' claims are typical of the claims of the members of the Class they seek to represent, because the factual and legal bases of Defendant's liability to Plaintiffs and the other members are the same, and because Defendant's conduct has resulted in similar injuries to Plaintiffs and to the Class. As alleged herein, Plaintiffs and the Class have all suffered damages as a result of Defendant's BIPA violations and common law transgressions.

41. There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members. Common questions for the Class include, but are not limited to, the following:

- a. Whether Defendant's timekeeping technology and associated conduct is subject to BIPA;
- b. Whether Defendant made available to the public a written policy that establishes a retention schedule and guidelines for destroying biometrics;
- c. Whether Defendant obtained a written and executed release from the Class before capturing, collecting, or otherwise obtaining their biometrics;
- d. Whether Defendant provided a written disclosure that explains the specific purposes, and the length of time, for which biometrics were being collected, stored and used before taking such biometrics;
- e. Whether Defendant's conduct violates BIPA;

- f. Whether Defendant's conduct is negligent;
- g. Whether Defendant's violations of the BIPA are willful or reckless; and
- h. Whether Plaintiffs and the Class are entitled to damages and injunctive relief;
- i. Whether Defendant provided a written disclosure that explains the specific purposes, and the length of time, for which biometrics were being collected, stored and used before taking such biometrics.

42. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

43. Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Class he seeks to represent. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiffs nor their counsel has any interest adverse to those of the other members of the Class.

44. Defendant has acted and failed to act on grounds generally applicable to the Plaintiffs and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

45. Defendant is a private entity under BIPA.

46. BIPA requires private entities, such as Defendant, to obtain informed written consent from individuals before acquiring their biometric information. Specifically, BIPA makes it unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or

customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject ... in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject ... in writing of the specific purpose and length of for which a biometric identifier or biometric information is being captured, collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information". 740 ILCS 14/15(b).

47. Illinois's BIPA also requires that private entities in possession of biometric identifiers and/or biometric information establish and maintain a publicly available retention policy. Entities which possess biometric identifiers or information must (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric information (entities may not retain biometric information longer than three years after the last interaction with the individual); and (ii) adhere to the publicly posted retention and deletion schedule.

48. Plaintiffs and the other Class members have had their "biometric identifiers", namely their fingerprints, collected, captured, received or otherwise obtained by Defendant and/or its technology. Plaintiffs and the other Class members' biometric identifiers were also used to identify them, and therefore constitute "biometric information" as defined by BIPA. 740 ILCS 14/10

49. Each instance Plaintiffs and the other Class members had their fingerprints scanned into Defendant's biometric devices, Defendant and/or its technology captured, collected, stored, and/or used Plaintiffs and the other Class members' biometric identifiers or biometric information without valid consent and without complying with and, thus, in violation of BIPA.

50. Defendant's practice with respect to capturing, collecting, storing, and using biometrics fails to comply with applicable BIPA requirements:

- a. Defendant failed to inform Plaintiffs and the members of the Class in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);
- b. Defendant failed to inform Plaintiffs and the Class in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);
- c. Defendant failed to inform Plaintiffs and the Class in writing the specific length of term their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);
- d. Defendant failed to obtain a written release, as required by 740 ILCS 14/15(b)(3);
- e. Defendant failed to provide a publicly available retention schedule detailing the length of time for which the biometrics are stored and/or guidelines for permanently destroying the biometrics they store, as required by 740 ILCS 14/15(a); and/or
- f. Defendant failed to obtain informed consent to disclose or disseminate the Class' biometrics, as required by 740 ILCS 14/15(d)(1).

51. By designing and operating an employee timekeeping system which uses biometrics that was devoid of the privacy protections required by BIPA, Defendant profited from Plaintiffs and the Class members' biometric identifiers and biometric information in violation of 740 ILCS 14/15(c). Defendant knew, or was reckless in not knowing, that the biometric systems it was selling, maintaining, and/or servicing would be subject to the provisions of BIPA yet wholly failed to comply with the statute.

52. By capturing, collecting, storing, using, and disseminating Plaintiffs and the Class members' biometrics as described herein, Defendant denied Plaintiffs and the Class their right to statutorily-required information and violated their respective rights to biometric information privacy, as set forth in the BIPA.

53. Had Defendant informed Plaintiffs that he was not being provided with the required information regarding his biometrics and the biometric timekeeping program it was providing as required by law, or that the biometric technology it was providing was not legally compliant, they may not have worked in the subject employment conditions or agreed to provide his biometrics without additional compensation.

54. Further, had Defendant provided Plaintiffs with all required disclosures, they at least would have been able to make an informed decision concerning material facts of the work environment, including whether the rate of pay and opportunity cost justified participating in the biometric timekeeping program.

55. The BIPA provides for statutory damages of \$5,000 for each willful and/or reckless violation of the BIPA and, alternatively, damages of \$1,000 for each negligent violation of the BIPA. 740 ILCS 14/20(1).

56. Defendant's violations of the BIPA, as set forth herein, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with BIPA.

Wherefore, Plaintiffs Jacinta Castro and Serapio Chavez, on behalf of themselves and the proposed Class, prays for:

a. the certification of the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;

b. a declaration that Defendant's actions violate BIPA;

c. an award of injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with the BIPA requirements for the capture and collection of biometrics, as well as requiring Defendant to comply with the written retention policy requirements of 740 ILCS 14/15(a);

d. an award of statutory damages of \$5,000 for each willful and/or reckless violation of BIPA, pursuant to 740 ILCS 14/20(1), more specifically, an award of \$5,000 for each and every time Defendant took Plaintiff's and the Class's biometric information;

e. an award of statutory damages of \$1,000 for each negligent violation of BIPA, pursuant to 740 ILCS 14/20(3), more specifically, an award of \$1,000 for each and every time Defendant took Plaintiff's and the Class's biometric information;

f. an award of reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3); and/or

g. Grant such additional or alternative relief as this Honorable Court deems just and proper.

Jacinta Castro and Serapio Chavez
Individually And On Behalf Of
Themselves And All Other Similarly
Situated Persons, Known And
Unknown,



By, one of their attorneys

Daniel Schlade (#6273008)
James Dore (#6296265)
Justicia Laboral, LLC
6232 N. Pulaski, #300
Chicago, IL 60646
773-550-3775
dschlade@justicialaboral.com
jdore@justicialaboral.com

